Remarks – General

The applicants have rewritten the claims to define the invention more particularly and distinctly so as to overcome the technical rejections and define the invention as patentable over the prior art.

Clarification on the Invention Disclosed in Zeng et al US Patent No 6,505,299

The methods and apparatus described in Zeng et al in US Patent No. 6,505,299 (hereinafter '299) for the encryption and decryption of digital images have, as a necessary step, the application of a space-frequency transform prior to the encryption operation ('299 col. 3, lines 25-36).

The space-frequency transform results in a transform coefficient map ('299 col. 3, lines 25-28). The coefficients in the transform coefficient map contain spatial frequency and spatial location information ('299 col. 4, 41-44). They are derived from a discrete cosine transform (DCT) described in '299 col. 4, line 66 through col. 5, line 14. The coefficients in the map are scrambled through an encryption operation. ('299 col. 3, lines 28-35).

The decryption operation descrambles the coefficients in the transform coefficient map ('299 col. 3, lines 58-60).

Zeng et al in '299 col 4, lines 40-45, describe space-frequency transforms as representations of digital images in terms of spatial and frequency data. Zeng et al includes the examples, block-based spatial frequency transforms and wavelet transforms.

Those skilled in the art recognize space-frequency transforms as operations to compress digital images, and the transform coefficient maps as block-based compressed images. The result is that the images may be stored and transmitted in fewer computer bytes than if the images were not compressed.

Those skilled in the art also recognize that the coefficients are non-algebraic in nature and are derived in the block-based compression of the images in '299. They are used to reconstruct the image from the block-based, transform coefficient map.

To summarize, Zeng et al in '299 teach an invention where the encryption and decryption operations are applied to image data that is first transformed into a map containing frequency and spatial data. The encryption and decryption steps operate on and are dependent on the transform coefficient map, not the raw image itself.

Major Differences between the Invention Disclosed in '299 and the Present Invention

The patent described in '299 and the present invention are fundamentally different.

First in the present invention, the encryption is applied to the raw image itself as opposed to a transform coefficient map as taught in '299. The decryption in the present invention results in the raw image, whereas in '299 it results in a transform coefficient map.

It was argued in the previous section that the space-frequency transform in '299 has the effect of compressing the image.

The patent application page 4, lines 3-5 states

> "Currently, classical encryption techniques are being applied to the problem, but they are inadequate for two reasons. First, they are not fast enough for real-time decryption on a frame-by-frame basis."

Indeed, one of the problems that the present invention addresses is the speed of encryption and decryption. Adding steps to transform the images by the methods taught in '299 would slow down the methods taught in the present invention, and would be

counter-productive to the purpose of the present invention. Thus, '299 teaches away from the present invention.

Throughout the specification, examples, preferred embodiments, and claims of the present invention, the novel cryptographic methods are applied to raw uncompressed images.

Second, the bits representing the raw image in computer code are encrypted. On the other hand, the coefficients in the transform coefficient map are encrypted in '299. The coefficients have been described in the previous section as numbers which contain both spatial and frequency data and are non-algebraic in nature.

The coefficients in the present invention are used to define algebraic equations, such as equation (1) and equation (11) in the patent application. The coefficients in the present invention are not encrypted as they are in '299.

Third in the embodiments with the radiometric expressions, the bitwise expressions which are combined with the data blocks are derived from the raw image itself. The radiometric expressions, and thus the bitwise expressions, derive from unique and novel application of image science principles.

In '299, the coefficients in the transform coefficient map are encrypted with methods, such as shuffling and scrambling ('299 col. 4, lines 51-54) that are unrelated to the raw image data.

The Rejection of Claims 1-28 Based on Zeng et al US Patent No. 6,505,299 is Overcome

In the last office action, claims 1-28 were rejected under 35 U.S.C. 102(e) as being anticipated by Zeng et al in '299. The claims were rewritten to define the invention more particularly, distinctly, and as patentable over '299. The applicants request

reconsideration of this rejection as now applicable to claims 29-56 for the following reasons:

(1) The invention described in '299 is substantially different from the features in claims 29-56.

(2) The invention described in '299 teaches away from the features in claims 29-56.

(3) Claims 29-56 are not anticipated from '299.

Independent Claim 29 is Patentable Over '299

Independent claim 1, which was rejected in the office action based on numerous references to '299, is now claim 29 with the following changes:

> **A method for encrypting and decrypting raw digital images comprising the steps of**
>
> **using a cyclotomic polynomial to generate an encrypting algebraic transform;**
>
> **partitioning said raw digital images into data blocks;**
>
> **calculating encrypted data blocks with said encrypting algebraic transform and said data blocks; and**
>
> **calculating decrypted data blocks with the inverse of said encrypting algebraic transform and said encrypted data blocks.**

The word, "raw," is used to describe the digital images and distinguish them from the image data that is encrypted in '299.

The image data in '299 that is encrypted is a transform coefficient map ('299 col. 3, lines 25-35). The transform coefficient map is generated with a space-frequency transform ('299 col. 3 lines 25-27). The transform coefficient map is clearly not a raw image itself because it contains space-frequency transform coefficients ('299 col.4 lines 45-46).

The preferred space-frequency transforms are identified as DCT-based and wavelet-based ('299 col. 4 lines 32-35). Those skilled in the art readily recognize these transforms as those used for compressing images.

Indeed, the inventors of '299 teach a method where the compressed and transformed image data is encrypted.

In the present invention, raw images, not transformed images, are encrypted. Raw images consist of pixels, which encode the light intensity of each portion of an image scene. The patent application page 16, lines 9-12 states

> "Digital images are arrays of small entities called pixels. Each pixel represents a portion of the image scene. When the digital images are color digital images, each pixel, typically, has three values representing the three components, red, green, and blue, which together represent the color of that portion of the scene."

The specification was amended to add the following statement at page 16, line 10 to clarify the nature of the image data that is encrypted.

> "Such digital images are also known in the art as raw digital images."

The preferred embodiments and the Examples 1-6 in the specification are all with raw images. Also, none of the images in the preferred embodiments and in Examples 1-6 are compressed by any technique.

The first step is now "using a cyclotomic polynomial to generate an encrypting algebraic transform." The word, "algebraic," is used to describe the transform and distinguish it from the transform disclosed in '299 col. 3, lines 25-36. The transform in '299 is a "space-frequency transform (col 3. line 28). Examples are "block-based spatial frequency transforms and wavelet transforms (col. 4, lines 43-44).

The transform in the present invention is an algebraic form. The patent application on page 8, lines 8-12, states

> "In step 102, the encrypting transform is generated, wherein the choice is made as to the form of the encrypting transform and the mathematical equation to represent the encrypting transform. For instance, the choice is made to use a certain mathematical curve type such as a polynomial curve, an elliptical curve, or a cyclotomic polynomial curve as the encrypting transform."

Cyclotomic polynomial curves are recognized by those skilled in the art as being fundamentally algebraic in nature. The specification was amended to add the following statement at page 8, line 12 to clarify the nature of the transform.

> "It is understood from these examples that the form of the encrypting transform is fundamentally algebraic."

This is in contrast to the encryption step being applied to transformed coefficient map containing frequency and spatial data in '299. Note that '299 teaches away from the present invention in this regard.

The step, "transmitting said encrypted data blocks," that was in claim 1 was removed.

Dependent Claims 30-32 are Patentable Over '299

Dependent claims 2, 3, and 4 were rejected in the office action with reference to '299 col. 3, lines 23-36.

Claim 2 is now claim 30 with the following changes.

> **The method of claim 29, wherein said using step includes the step of determining a mathematical algebraic equation representing said encrypting algebraic transform, and said mathematical algebraic equation is said cyclotomic polynomial.**

The word, "algebraic," was added to describe the mathematical equation. Determining the mathematical equation is discussed in the patent application page 8, lines 10-14 as follows:

> "..... the choice is made to use a certain mathematical curve type such as a polynomial curve, an elliptical curve, or a cyclotomic polynomial curve as the encrypting transform. After this choice is completed, an equation is determined by choosing coefficients for the mathematical equation representing the encrypting transform."

As established with the rationale for claim 29, the mathematical curve type is fundamentally algebraic.

The form of the cyclotomic polynomials that are used in this invention is shown in equation (11) in the patent application and is clear to those skilled in the art as algebraic. Further, examples 3 and 4 illustrate the use of cyclotomic polynomials. Equation (18), which is used in examples 3 and 4, is a cyclotomic polynomial and is clearly algebraic.

FIG. 2, which is also used in examples 3 and 4, illustrates the unit circle, a well-known concept in abstract algebra textbooks.

Claim 3 is now claim 31 with the following changes.

> **The method of claim 29, wherein said using step includes the step of determining a mathematical algebraic equation representing said encrypting algebraic transform, and the coefficients of said mathematical algebraic equation are calculated with said cyclotomic polynomial.**

The word, "algebraic," was added to describe the mathematical equation. The justification is the same rationale as for claim 30.

The coefficients in claim 31 are fundamentally different than the coefficients mentioned in '299 col. 3, lines 30-35. The coefficients in '299 are components of the transform coefficient map. They contain spatial and frequency information about the image and are inherently derived from the image. Also, they are encrypted by scrambling and shuffling as described in '299 col. 6 lines 39-63.

The coefficients in the present invention are from algebraic equations. They contain no spatial and frequency information about the image and are not inherently related to the image. Also, they are not scrambled or shuffled as in '299. The patent application on page 8, lines 12-14 states

> "After this choice is completed, an equation is determined by choosing coefficients for the mathematical equation representing the encrypting transform."

The patent application on page 10, lines 12-15 states

> "In one example of using elliptical curves for cryptography, the coefficients, K_1 and K_2, may be chosen in step 102 in FIG. 1. They must be chosen prudently for maximum security and maximum computational efficiency. They may be numerical based or polynomial based."

The patent application on page 14, lines 17-18 states

> "One embodiment of using cyclotomic polynomials in cryptographic applications is in the calculation of the coefficient, K_2, when using elliptical curve equations."

The specification clearly describes coefficients as those used in algebraic equations. In this embodiment, coefficients of elliptical curves are defined by cyclotomic polynomials. The coefficients are not used as they are in transform coefficient maps as in '299.

Claim 4 is now claim 32 with the following changes.

> **The method of claim 29, wherein said using step includes the step of determining a mathematical algebraic equation representing said encrypting algebraic transform, and said mathematical algebraic equation is modulo said cyclotomic polynomial.**

The word, "algebraic," was added to describe the mathematical equation. The justification is the same rationale as for claims 30 and 31.

Dependent Claims 33-35 are Patentable Over '299

Dependent claims 5, 6, and 7 were rejected in the office action with reference to '299 col. 5, lines 1-15.

Claim 5 is now claim 33 with the following changes.

The method of claim 30, wherein said raw digital images are raw color digital images.

Claim 6 is now claim 34 with the following changes.

The method of claim 31, wherein said raw digital images are raw color digital images.

Claim 7 is now claim 35 with the following changes.

The method of claim 32, wherein said raw digital images are raw color digital images.

The word, "raw," is used to describe the color digital images and distinguish them from the image data that is encrypted in '299. The rationale is the same as that regarding claim 29.

Dependent Claims 36-38 are Patentable Over '299

Dependent claims 8, 9, and 10 were rejected in the office action with reference to '299 col. 1, lines 5-21.

Claim 8 is now claim 36 with the following changes.

The method of claim 33, wherein said raw color digital images comprise a set of raw images in digital cinema.

Claim 9 is now claim 37 with the following changes.

The method of claim 34, wherein said raw color digital images comprise a set of raw images in digital cinema.

Claim 10 is now claim 38 with the following changes.

The method of claim 35, wherein said raw color digital images comprise a set of raw images in digital cinema.

The word, "raw," is used to describe the images in digital cinema and distinguish them from the image data that is encrypted in '299. The rationale is the same as that regarding claim 29.

Independent Claim 39 is Patentable Over '299

Independent claim 11, which was rejected in the office action based on numerous references to '299, is now claim 39 with the following changes:

A method for encrypting and decrypting raw digital images comprising the steps of:

using a radiometric expression derived from said raw digital images to generate a bit sequence;

partitioning said raw digital images into data blocks with length equal to the length of said bit sequence;

combining said bit sequence and said data blocks to form encrypted data blocks; and

separating said bit sequence and said data blocks to form unencrypted data blocks.

The word, "raw," is used to describe the digital images and distinguish them from the image data that is encrypted in '299. The rationale is the same as that regarding claim 29.

The first step now states "using a radiometric expression derived from said raw digital images to generate a bit sequence." The new wording more particularly defines claim 39 over the previous wording in claim 11.

The patent application on page 16, lines 20-22 states

> "In this invention, the red, green and blue values are converted to a color space known in the art as CIE XYZ space (Poynton, pages 147 – 148)."

and on page 17, lines 6-7 states

> "Once in CIE XYZ space, the color of that the pixel is broken down into the metameric components referred to as a fundamental metamer and a black metamer."

In the present invention, the color components (red, green, and blue) of a pixel are converted to a radiometric expression, which is used to generate a bit sequence.

The phrase, "bit sequence," is used to describe that which is generated with a radiometric expression. It underscores the difference between this claim and the transform which is disclosed in '299 col. 3, lines 25-36. The transforms are identified as space-frequency transforms ('299 col. line 26), which converts images into a set of coefficients, each of which contain frequency and spatial information ('299 col. 4 lines 41-42).

The patent application on page 19, lines 3-6 states

> "Any one or any combination of the floating point numbers of the metamers and the radiometric function, referred to as the radiometric expression, is used in the cryptographic system. The floating point numbers in binary can be concatenated together to form a large precision integer."

The large precision integer is one example of a sequence of bits, or bit sequence. The specification was amended to add the following statement at page 19, line 6.

> "It will be recognized that the floating point numbers can be concatenated to form sequences of bits with any length."

The using step of this claim results in a bit sequence, such as a high precision integer, as opposed to the transform in '299 which results in a transform coefficient map.

The patent application page 20, lines 7-8 states

> "One advantage in the use of metameric components and the radiometric function is that, they are derived from the image data itself instead of being derived independently."

Note that the radiometric expression is derived from the raw image itself. There is no mention anywhere in '299 of a step comparable to the using step in claim 39.

The phrase, "with length equal to the length of said bit sequence," was added to more particularly define the partitioning step. Rejection to this step was based on '299 col. 3, lines 44-53.

In '299, the encryption buffer accepts transformed image data ('299 col. 3, lines 45-47). The transformed image data is a transform coefficient map ('299 col. 3, line 27). The

encryption that is taught is with the coefficients of the transform coefficient map ('299 col. 6, lines 49-53).

The patent application page 19, lines 15-20 states

> "The preferred embodiment is where any one or combination of the floating point numbers of the radiometric expression are mathematically combined with the data blocks. The binary form of the radiometric expression, called the bitwise expression is, for instance, added or multiplied with the data block. The embodiment that is more preferred is combining the bitwise expression with the data blocks with an exclusive-or mathematical operation, common in the field of computer science."

Whereas the inventors in the '299 patent teach a step that partitions the image into an transform coefficient map, the present invention teaches a step that combines the bitwise expression with the radiometric expression.

The step, "transmitting said encrypted data blocks," that was in claim 11 was removed.

Dependent Claim 40 is Patentable Over '299

Dependent claim 12 was rejected in the office action with reference to '299 col. 4, lines 39-49.

Claim 12 is now claim 40.

The inventors respectfully request that dependent claim 40 be reconsidered for acceptance. As has been sufficiently argued with independent claims 29 and 39, '299 col. 4, lines 39-49 teach a method of using a space-frequency transform to convert an image to an transform coefficient map, a step which teaches away from the present invention.

Dependent Claims 41 and 44 are Patentable Over '299

Dependent claims 13 and 16 were rejected in the office action with reference to '299 col. 5, lines 1-15.

Claim 13 is now claim 41 with the following changes.

The method of claim 40, wherein said raw digital images are raw color digital images.

Claim 16 is now claim 44 with the following changes.

The method of claim 43, wherein said raw digital images are raw color digital images.

The word, "raw," is used to describe the color digital images and distinguish them from the image data that is encrypted in '299. The rationale is the same as that regarding claim 29.

Dependent Claims 42 and 45 are Patentable Over '299

Dependent claims 14 and 17 were rejected in the office action with reference to '299 col. 1, lines 5-21.

Claim 14 is now claim 42 with the following changes.

The method of claim 41, wherein said raw color digital images comprise a set of raw images in digital cinema.

Claim 17 is now claim 45 with the following changes.

The method of claim 44, wherein said raw color digital images comprise a set of raw images in digital cinema.

The word, "raw," is used to describe the images in digital cinema and distinguish them from the image data that is encrypted in '299. The rationale is the same as that regarding claim 29.

Dependent Claims 43 is Patentable Over '299

Dependent claim 15 was rejected in the office action with reference to '299 col. 3, lines 23-36.

Claim 15 is now claim 43.

The inventors respectfully request that dependent claim 43 be reconsidered for acceptance. It has been sufficiently argued that '299 col. 3, lines 23-36 teaches away from the present invention.

Dependent Claims 46 is Patentable Over '299

Dependent claim 18 was rejected in the office action with reference to '299 col. 4, line 66 through col. 5, line 26.

Claim 18 is now claim 46.

The inventors respectfully request that dependent claim 46 be reconsidered for acceptance.

The inventors in '299 use the luma and chroma components of compressed images ('299 col. 5, lines 3-7). Luma and chroma components are widely used in the video industry. A pixel is described with three numbers, one luma and two chroma. '299 makes no reference anywhere that the luma and chroma numbers are to be understood any other way than what is widely understood in the art.

The patent application page 18, line 20 through page 19, line 3 states

> "In this invention, a pixel's red, green, and blue values are converted to its respective CIE XYZ values after which the respective fundamental metamer, a component black metamer, and a component radiometric function are calculated. The metamers and radiometric function are preferably stored in the computer memory as floating point binary numbers. Preferably, 31 points are used to represent the visible spectrum, so there will be 31 floating point numbers for each of the metamers and the radiometric function. Any one or any combination of the floating point numbers of the metamers and the radiometric function, referred to as the radiometric expression, is used in the cryptographic system."

From this passage in the present invention, one set of pixel values translate into radiometric expressions. The radiometric expressions are functions that can be plotted on an intensity versus wavelength plots, such as shown in FIG. 3.

The use of radiometric expressions is unique and novel in the field of cryptography and are fundamentally different from the teaching of luma and chroma in '299.

Dependent Claim 47 is Patentable Over '299

Dependent claim 19 was rejected in the office action with reference to '299 col. 4, line 66 through col. 5, line 26.

Claim 19 is now claim 47.

The inventors respectfully request that dependent claim 47 be reconsidered for acceptance. The argument for acceptance is identical to that for claim 46.

Dependent Claim 48 is Patentable Over '299

Dependent claim 20 was rejected in the office action with reference to '299 col. 4, line 66 through col. 5, line 26.

Claim 20 is now claim 48.

The inventors respectfully request that dependent claim 48 be reconsidered for acceptance. The argument for acceptance is identical to that for claim 46.

Independent Claim 49 is Patentable Over '299

Independent claim 21, which was rejected in the office action based on numerous references to '299, is now claim 49 with the following changes:

> **A method for encrypting and decrypting raw digital images comprising the steps of:**
>
> **using a cyclotomic polynomial to generate an encrypting algebraic transform;**
>
> **partitioning said raw digital images into data blocks;**
>
> **calculating encrypted data blocks with said encrypting algebraic transform, said data blocks and a radiometric expression derived from said raw digital images; and**

calculating decrypted data blocks with the inverse of said encrypting algebraic transform and said encrypted data blocks.

The word, "raw," is used to describe the digital images and distinguish them from the image data that is encrypted in '299. The rationale is the same as that regarding claim 29.

The first step now states "using a cyclotomic polynomial to generate an encrypting algebraic transform." The word, "algebraic," is used to describe the transform and distinguish it from the transform disclosed in '299 col. 3, lines 25-36. The rationale is the same as that regarding claim 29.

The phrase, "derived from said raw digital images," was added to the calculating encrypted data blocks step. The patent application on page 16, lines 20-22 states

> "In this invention, the red, green and blue values are converted to a color space known in the art as CIE XYZ space (Poynton, pages 147 – 148)."

and on page 17, lines 6-7 states

> "Once in CIE XYZ space, the color of that the pixel is broken down into the metameric components referred to as a fundamental metamer and a black metamer."

In the present invention, the color components (red, green, and blue) of a pixel are converted to a radiometric expression, which is used to calculate the encrypted data block.

The patent application page 20, lines 7-8 states

> "One advantage in the use of metameric components and the radiometric function is that, they are derived from the image data itself instead of being derived independently."

Note that the radiometric expression is derived from the raw image itself. There is no mention anywhere in '299 of a step comparable to the calculating encrypted data block step in claim 49.

The step, "transmitting said encrypted data blocks," that was in claim 21 was removed.

Dependent Claim 50 is Patentable Over '299

Dependent claim 22 was rejected in the office action with reference to '299 col. 4, line 66 through col. 5, line 26.

Claim 22 is now claim 50.

The inventors respectfully request that dependent claim 50 be reconsidered for acceptance. The argument for acceptance is identical to that for claim 46.

Dependent Claim 51 is Patentable Over '299

Dependent claim 23 was rejected in the office action with reference to '299 col. 9, lines 11-38.

Claim 23 is now claim 51

.The exclusive-or operation in '299 is applied to the coefficients of the transform coefficient map ('299 col. 9, lines 11-38). The inventors of the present invention have sufficiently argued with regards to claim 31 that these coefficients in '299 are radically different than those in the present invention.

Dependent Claim 52 is Patentable Over '299

Dependent claim 24 was rejected in the office action with reference to '299 col. 5, lines 1-15.

Claim 24 is now claim 52 with the following changes.

The method of claim 51, wherein said raw digital images are raw color digital images.

The word, "raw," is used to describe the color digital images and distinguish them from the image data that is encrypted in '299. The rationale is the same as that regarding claim 29.

Dependent Claim 53 is Patentable Over '299

Dependent claim 25 was rejected in the office action with reference to '299 col. 1, lines 5-21.
Claim 25 is now claim 53 with the following changes.

The method of claim 52, wherein said raw color digital images comprise a set of raw images in digital cinema.

The word, "raw," is used to describe the images in digital cinema and distinguish them from the image data that is encrypted in '299. The rationale is the same as that regarding claim 29.

Dependent Claims 54-56 are Patentable Over '299

Dependent claims 26, 27, and 28 were rejected in the office action with reference to '299 col. 4, line 66 through col. 5, line 26.

Claims 26, 27, and 28 are now claims 54, 55, and 56.

The inventors respectfully request that dependent claims 54-56 be reconsidered for acceptance. The argument for acceptance is identical to that for claim 46.

Conclusions

For all the above reasons, the applicants submit that the specification and claims are now in proper form, and the claims all define patentably over the prior art. Therefore, they submit that this application is now in condition for allowance, which action they respectfully solicit.

Very respectfully,

Michael P. Keyes Philip E. Cannata

----------Applicants Pro Se----------

8917 Joachim Ln.
Austin, TX 78717
Tel (512) 671-3587

Certificate of mailing: I certify on the date below this document will be deposited with the U.S. Postal Service in an envelope addressed to: "Box NON-FEE AMENDMENTS, Assistant Commissioner for Patents, Washington D.C. 20231

2005 February 28 Michael P. Keyes